Het verband tussen publiek belang en ontwerp bij het internet der dingen

den Butter, F.A.G.; den Butter, G.G.J.

published in
Beleid en Maatschappij
2016

document version
Publisher's PDF, also known as Version of record

Het verband tussen publiek belang en ontwerp bij het internet der dingen*

*Frank Den Butter & Gijs Den Butter***

Het internet der dingen levert een schat aan gegevens (big data) op over persoonlijk gedrag. Bij de benutting van deze gegevens is sprake van verschillende vormen van publiek belang waarvoor de overheid borgingsmechanismen in werking dient te stellen. Daarbij gaat het enerzijds om goede beschikbaarheid van gegevens, om het opheffen van informatieasymmetrie als vorm van marktfalen, en anderzijds om het bieden van rechtsbescherming ten aanzien van veiligheid en privacy. In dit artikel bespreken wij hoe vanuit de principaal/agentbenadering van regelgeving ten aanzien van borging van de verschillende onderdelen van het publiek belang het ontwerpproces van applicaties en systemen in het internet der dingen het best kan worden vormgegeven. Het voorbeeld van de slimme thermostaat Toon® leert hoe de samenwerking tussen ontwerpers en software-ingenieurs heeft bijgedragen aan zowel een goede bescherming van de gegevens als een mogelijke prikkel tot energiebesparing.

Inleiding

De in 2002 door Steven Spielberg geregisseerde film *Minority Report* schetst een bijzonder toekomstbeeld. Het is 2054, en de door Tom Cruise gespeelde politieinspecteur John Anderton is verantwoordelijk voor de arrestatie van toekomstige moordenaars voordat ze de moord hebben gepleegd. De irisscanner wordt in die wereld als algemeen identificatiemiddel gebruikt. In deze film komt een korte scene voor die in 2002 nog een verre toekomst leek, maar die nu profetisch blijkt te zijn.[1] Wanneer John Anderton door een winkelcentrum loopt, hoort hij overal zijn naam en krijgt hij in etalages en via doorzichtige beeldschermen allerlei aanbiedingen die zijn afgestemd op zijn koopgedrag en daaruit afgeleide smaak. In zekere zin is deze vorm van gepersonifieerde reclame al werkelijkheid, zij het dat de persoonsidentificatie niet via overal opgestelde irisscanners plaatsvindt.
Vooralsnog verschijnen de speciale aanbiedingen op de computerschermen van degenen die via allerhande websites en zoekmachines informatie over hun voorkeuren hebben achtergelaten. Voor aanbieders van consumentenproducten en -diensten is deze informatie veel geld waard. Dat werd nog eens duidelijk geïllustreerd toen Hans Hagenaars, directeur Particulieren van ING Bank, in een inter-

* De schrijvers zijn dank verschuldigd aan een referent voor kritische opmerkingen bij een eerdere versie van dit artikel.

** Prof. dr. Frank den Butter is hoogleraar algemene economie aan de Vrije Universiteit Amsterdam. f.a.g.den.butter@vu.nl Ir. Gijs den Butter is MSc 'Strategic Product Design' aan de Technische Universiteit Delft en CEO van Adjuvo Motion, een start-up bij YesDelft! die een robotische brace voor revalidatie op de markt brengt. g.butter@adjuvomotion.com

view aan *Het Financieele Dagblad* van 10 maart 2014 bekendmaakte dat ING het plan had om klantgegevens commercieel te gebruiken ten behoeve van aanbiedingen door andere bedrijven. Het bleek nog een brug te ver en leverde een stroom van verontwaardiging op tegen de inbreuk op de privacy en tegen het feit dat de bank met het plan het publiek belang van het betaalverkeer veronachtzaamde. In reactie hierop zijn de banken in januari 2015 een lobby begonnen tegen bedrijven zoals Google en Apple om te verhinderen dat deze via betaalapplicaties toegang krijgen tot rekeninggegevens van Nederlanders en deze wel voor reclamedoeleinden kunnen gaan gebruiken. Dat wordt nu als oneerlijke concurrentie gezien. Vanuit een soortgelijke lobby pleitte Diana Janssen, voorzitster van DDMA, de branchevereniging voor datagedreven marketing, bij de opening van de Amsterdam Privacy Week in oktober 2015 voor een versoepeling van de privacywetgeving bij het door bedrijven verzamelen en verkopen van gegevens van hun klanten.

Het verzamelen van grote hoeveelheden gegevens, zogenaamde 'big data', met persoonlijke informatie blijft niet beperkt tot het internetgebruik via thuiscomputers en laptops. Tegenwoordig zijn er veel meer manieren waarop via slimme apparaten gegevens op internet worden uitgewisseld en vervolgens voor geïnteresseerde aanbieders van diensten beschikbaar komen. Denk aan het feit dat velen van ons een mobiele telefoon hebben die we overal gebruiken om te communiceren en informatie uit te wisselen. Via het gps in de telefoons weten we waar we zelf zijn, maar ook waar we heen kunnen gaan voor bijvoorbeeld een goed restaurant in de buurt of voor de bus naar het station. De mobiele applicatie van het verhuurbedrijf van elektrische stadsauto's, Car2Go, vertelt waar de dichtstbijzijnde huurauto geparkeerd staat. Vanuit de auto of het kantoor kunnen we de verwarming hoger of lager zetten en, indien we willen, kan de supermarkt bijhouden wat we in de koelkast hebben en eventueel aanvullingen suggereren. Met al deze gegevens via internet geven we informatie over onze gedragspatronen en ons reilen en zeilen, waarvan dienstverleners al dan niet geanonimiseerd gebruik kunnen maken. Deze bronverschaffing van informatie wordt samengevat als het *internet der dingen* (Internet of Things).

Het staat buiten kijf dat het internet der dingen, en de informatie die erdoor beschikbaar komt, ingrijpende invloed kan hebben op onze leefwijze. Het doembeeld dat *Minority Report* voor John Alderton schetst, hoeft dan nog geen werkelijkheid te worden; de sturing die het internet der dingen aan ons leven kan geven, gaat wel in die richting. De vraag is in hoeverre de overheid zich met het internet der dingen moet bemoeien, en zo ja, waarom en in welke vorm die bemoeienis zou moeten plaatsvinden. Anders gezegd is het de vraag wat het publiek belang van het internet der dingen is, en op welke wijze de overheid zou moeten zorgen dat dit publiek belang wordt geborgd. In dit artikel wordt deze vraag toegespitst op de relatie tussen regelgeving door de overheid en de manier waarop in het ontwerpproces van applicaties rekening moet worden gehouden met de borging van het publiek belang. De vraag bij deze toespitsing is dus hoe het ontwerpproces moet worden ingericht en wat de rol van de verschillende betrokkenen bij het ontwerpproces is, zodat de verschillende vormen van publiek belang bij het internet der dingen worden geborgd. Vanuit deze vraagstelling

wordt eerst een nadere aanduiding gegeven van wat het internet der dingen inhoudt en wat de mogelijke ontwikkelingen zijn. Vervolgens bespreken we wat in dit artikel onder publiek belang wordt verstaan en welke rol de overheid hierbij speelt. Daarbij wordt gefocust op de overheidsbemoeienis om de publieke belangen te borgen die in het kader van het internet der dingen spelen. Een belangrijk aspect daarbij is het gecompliceerde technische karakter van deze nieuwe wijze van het gebruik van internet voor gegevensverzameling. Er is sprake van een flinke informatieasymmetrie tussen de opdrachtgever, de ontwerper, de softwareontwikkelaar en de overheid bij de ontwikkeling van nieuwe internetapplicaties. Vervolgens wordt deze gelaagde, of gestaffelde, principaal-agentrelatie besproken vanuit de praktijk van het industrieel ontwerpen. Ingezoomd wordt op een voorbeeld van benutting van het internet der dingen, namelijk de slimme thermostaat Toon® van Eneco. Hier is sprake van enerzijds een positief extern effect, voor zover het gebruik van Toon beoogt om gebruikers tot energiebesparing aan te zetten, maar anderzijds ook van de rechtsstatelijke randvoorwaarde van het voorkomen van misbruik en van privacybescherming bij het gebruik van de gegevens. Dit laatste vormt onderdeel van de rechtsbescherming die als collectief goed kan worden gezien. Ten slotte vatten we de bevindingen samen en geven we enkele beleidsaanbevelingen.

Internet der dingen

Bij het internet der dingen zijn de 'dingen' niet de mensen die via de computer of via de mobiele telefoon met elkaar communiceren. Het gaat juist om de apparaten die met sensoren en slimme interfaces zijn uitgerust en die met elkaar contact kunnen hebben en daarbij gegevens uitwisselen. Dit scenario van de moderne draadloze communicatie wint snel terrein. Voorzien wordt dat in de komende vijf jaar in de industrie het aantal machines dat met elkaar kan communiceren met 30 procent per jaar zal toenemen (McKinsey Global Institute, 2011). In 2020 zal 90 procent van alle auto's een internetverbinding hebben, terwijl dat in 2013 nog maar 10 procent was.[2] In 2020 zal iedereen gemiddeld beschikken over zeven verschillende apparaten die draadloos met elkaar verbonden zijn (Evans, 2011). Volgens Giusto en anderen (2010) is het basisidee van het internet der dingen:

> 'the pervasive presence around us of a variety of things or objects – such as Radio-Frequency IDentification (RFID) tags, sensors, actuators, mobile phones, etc. – which, through unique addressing schemes, are able to interact with each other and cooperate with their neighbors to reach common goals'.

Vanuit dat perspectief associëren Went en Kremer (2015) de met elkaar via internet communicerende apparaten met robots en spreken van het 'Internet of Robotic Things'.
Het spreekt voor zich dat deze nieuwe manier van interactie grote invloed heeft op de dagelijkse gang van zaken, een invloed die nog verder gaat dan de veranderingen die het gebruik van de sociale media nu al op ons gedrag heeft. Eenieder

die een mobiele telefoon bij zich heeft, geeft op elk moment informatie waar hij of zij zich bevindt. Via de wifi-verbinding is iedere telefoonbezitter overal traceerbaar. Irisscanners zijn daarbij niet nodig. Allerlei volgsystemen via sensoren, waaronder via RFID, hebben een snelle ontwikkeling van het internet der dingen mogelijk gemaakt. Voorwerpen die zijn voorzien van identificatiemiddelen, kunnen overal op afstand beheerd of bestuurd worden door mensen of computers. Het hoeft geen betoog dat dit een schat aan gegevens oplevert, en dus aan informatie, over de persoonlijke leefpatronen.

Publiek belang

Duidelijk is dat de overheid bij deze snelle en ingrijpende ontwikkeling niet aan de zijlijn kan staan. De vraag daarbij is welk publiek belang het internet der dingen met zich brengt waar de overheid voor borging dient te zorgen. Daartoe is nodig nader aan te duiden wat een publiek belang is. Vanuit een breed perspectief gaat het bij een publiek belang om overheidsbemoeienis die de welvaart bevordert. Butter (2011, 87) definieert daarbij een publiek belang als:

> 'een belang van ingezetenen van een land waarbij in een gegeven omstandigheid overheidsbemoeienis een grotere maatschappelijke welvaart kan opleveren dan wanneer er geen overheidsbemoeienis is'.

Deze definitie van het publiek belang combineert de bestuurskundige en bestuursrechtelijke interpretatie die de Wetenschappelijke Raad voor het Regeringsbeleid (WRR, 2000) aan dit begrip heeft gegeven met de economische interpretatie die onder meer is verwoord door Bovenberg en Teulings (1999) en Teulings, Bovenberg en Van Dalen (2003). Volgens de WRR is het aan de politiek om te bepalen wat een publiek belang is, terwijl vanuit het economisch perspectief de reparatie van allerlei vormen van marktfalen als een te borgen publiek belang moet worden gezien. Volgens de bovenstaande definitie is dus altijd overheidsbemoeienis nodig om via de borging van het publiek belang de welvaart te bevorderen. Wanneer de markt vanzelf een welvaartsoptimum oplevert, is er geen sprake van een publiek belang.

Deze definitie van publiek belang omvat alle redenen voor overheidsbemoeienis die de economische theorie van de collectieve sector (public economics) aangeeft. Het betreft hier, in de terminologie van het WRR-rapport (2000) de 'wat-vraag' van het publiek belang. Dat zijn in de eerste plaats kwesties van herverdeling en nivellering die vanuit politieke preferenties bepalend zijn voor de maatschappelijke welvaart. Herverdeling lijkt in verband met het internet der dingen overigens geen reden voor de overheid om zich om borging te bekommeren. Dit blijft dan ook hier verder buiten beschouwing.

Een tweede argument voor overheidsingrijpen betreft de taak van de overheid om te voorzien in collectieve en veelal ook semicollectieve goederen. In beginsel gaat dit om goederen en diensten die niet-rivaliserend en niet-uitsluitbaar zijn, en waarvan dus iedereen gebruik kan maken. Rechtsbescherming is vanuit dit oog-

punt een overheidstaak die als publiek belang moet worden opgevat. De argumentatie om de voorziening van collectieve goederen als een overheidstaak te zien is ontleend aan de economische theorie – private voorziening van deze goederen wordt gehinderd door free-riderschap –, maar de mate waarin de overheid collectieve voorzieningen verzorgt, vormt veelal onderdeel van het politieke debat. Zo is het bijvoorbeeld vooral een politieke kwestie welke toegang burgers tot de rechtspraak moeten krijgen. Evenzeer vraagt het een politiek oordeel hoeveel geld de overheid moet besteden aan defensie en om overstromingsgevaar te beperken. Opgemerkt zij dat de WRR (2011) het internet zelf als een collectief goed wil zien. Dit terwijl toegang tot internet weliswaar niet-rivaliserend, maar wel uitsluitbaar is. De WRR (2011) bepleit dat overheden, mede gezien het recht op vrije meningsuiting, toegang tot internet zo min mogelijk inperken.
Het derde argument voor overheidsbemoeienis is de reparatie van marktfalen. Dit betreft het internaliseren van externe effecten, het tegengaan van informatieasymmetrie en het bevorderen van concurrentie. Hier gaat het om een publiek belang waarbij de argumenten voor het waarom en hoe te borgen direct voortvloeien uit het economische gedachtegoed van de welvaartstheorie. Nadat is vastgesteld dat het daadwerkelijk om een publiek belang gaat (de wat-vraag), is de manier waarop de overheid voor borging zorgt (de hoe-vraag) vooral een technocratische kwestie. Economen en bestuurskundigen hebben hier ieder hun eigen redeneerwijzen. Uiteindelijk zullen de technocratische voorstellen wel weer onderdeel zijn van politieke besluitvorming (zie ook Schrijvers e.a., 2010; WRR, 2012).

Het publiek belang bij het internet der dingen

De bovenstaande aanduiding van het publiek belang en van de verschillende redenen voor de overheid om het publiek belang te borgen biedt een handvat voor de vraag welke bemoeienis de overheid met het internet der dingen dient te hebben. Het publiek belang bij het internet der dingen heeft een divers karakter.
Aan de ene kant dragen deze ontwikkeling en de daarbij beschikbare komende grote gegevensbestanden (de big data) bij aan de bevordering van de welvaart. Zo kunnen de gegevens gebruikt worden om de productie efficiënter te doen verlopen. Wanneer producenten van levensmiddelen of gebruiksgoederen precies weten wat de toekomstige behoefte is, betekent het minder verspilling aan voedsel en materiaal. In die zin kan het internet der dingen een bijdrage leveren aan een beter milieu. Daarnaast maakt het meer productdifferentiatie mogelijk, waarbij de te leveren goederen en diensten beter op de wensen van de eindgebruiker zijn afgestemd. Bedrijven kunnen ook persoonsgegevens gebruiken om risico's te managen (Bijlsma, Straathof & Zwart, 2014). Zo kan een bedrijf beter de kans op wanbetaling inschatten wanneer men over gegevens van het betalingsgedrag beschikt. Evenzeer kan een verzekeraar risicovolle klanten meer laten betalen dan klanten die op basis van hun persoonsgegevens minder risicovol gedrag vertonen. In geval van niet door de overheid gereguleerde verzekeringen biedt dit een welvaartsvoordeel, maar het kan ook betekenen, in geval van ziektekostenverzeke-

 doi: 10.5553/BenM/138900692016043001004 - Beleid en Maatschappij 2016 (43) 1

ringen in ons land, dat de risicosolidariteit onder druk komt te staan. Bomhof (2014) noemt een aantal technologiegedreven mogelijkheden, zoals de bepaling van de sterkte van dijken of de kansberekening op burn-outklachten, waar toepassing van big data maatschappelijk nuttig is gebleken.
Een andere toepassing van big data is dat leveranciers van content verschillende mogelijkheden kunnen bieden waarbij de auteursrechtelijke inkomsten van benutting van de content zijn geborgd. Een klant die bijvoorbeeld via HBO of Netflix een film wil bekijken, kan kiezen voor de dure optie, waarbij hij de film het hele jaar door kan bekijken, maar kan ook tegen een minder hoge prijs de film een week lang bekijken of kiezen voor een vaste vergoeding voor elke keer dat hij de film bekijkt.
Meer in het algemeen leveren de gegevens die langs deze weg worden verkregen informatie over het reilen en zeilen van de maatschappij op die in onderzoek nuttig kan worden gebruikt. De mogelijkheid om via het internet der dingen veel en nieuwe gegevens te verzamelen, vermindert de informatiekosten. De voorbeelden tonen dat de gegevens zowel voor de leverancier van producten en diensten als voor de consument waardevol kunnen zijn. Dat is de reden waarom met name producenten veel geld voor dit soort gegevens over hebben en waarom wel de verhandelbaarheid van persoonsgegevens wordt bepleit (Bijlsma e.a., 2014). Daarbij gaat het om een tweezijdige markt, waarbij de consumenten bij de verdeling van het welvaartsvoordeel gebaat zijn bij een goede concurrentie (Athey, 2014). Ten dele vallen deze productiviteitswinsten toe aan degenen die geïnvesteerd hebben in het verzamelen en toepassen van de big data. In die zin is sprake van goede marktwerking en gaat het hier niet om een publiek belang vanwege marktfalen. Ten dele hebben echter ook anderen baat bij deze ontwikkelingen – zie het voorbeeld van milieubesparing. In dat geval is wel sprake van positieve externe effecten en dus van een publiek belang, waarbij het een overheidstaak is deze ontwikkelingen te bevorderen.
Bovendien hebben dergelijke gegevens tot op zekere hoogte ook het karakter van een collectief goed, zodat de overheid zich vanuit dat perspectief op publiek belang moet inzetten voor openbaar gebruik van de gegevens. Dit sluit aan bij de rol van het Centraal Bureau voor de Statistiek (CBS): de gegevens die door dit bureau worden verzameld en ter beschikking gesteld, worden beschouwd als een collectief goed. Daarom is het de taak van de overheid om via het CBS in dit publiek belang te voorzien. Meer in het algemeen gaat het bij een toenemend gebruik van deze gegevens om borging van transparantie, toegankelijkheid en betrouwbaarheid van de gegevens (Raad voor de Leefomgeving en Infrastructuur, 2015, 42). Daarnaast kan de beschikbaarheid van big data, en vooral ook de snelheid waarmee informatie beschikbaar komt, bevorderlijk zijn voor de efficiëntie en effectiviteit van het overheidsbeleid zelf. Deze functie als collectief goed vormt dus een argument voor overheidsbemoeienis bij het verzamelen van big data.

Rechtsbescherming als publiek belang
De keerzijde van het op grote schaal verzamelen van gegevens over individueel gedrag en voorkeuren is dat het ook welvaartskosten met zich brengt. Een belangrijk aspect in dit verband is dat het een inbreuk op de privacy kan betekenen. In

die zin dient de overheid te zorgen voor de borging van handhaving van de privacy als onderdeel van de rechtsbescherming als publiek belang. Daarbij komt dat wanneer via sensoren en tags automatisch gegevens worden verzameld, de burger (of consument) zich er niet echt van bewust is dat hij veel persoonlijke informatie met zulke gegevens ter beschikking stelt. Dit is een informatieasymmetrie – of onvolledige informatie – waarbij overheidsbemoeienis nodig is om deze vorm van marktfalen op te heffen.
Privacybescherming heeft een stevige grondrechtelijke status (artikel 10 van de Grondwet). Daarbij dient de overheid er niet alleen voor te zorgen dat de eigen informatievoorziening de regels van de privacy respecteert, maar ook moet de overheid er garant voor staan dat dit recht tussen de burgers onderling wordt gehandhaafd. Met name deze laatste vorm van privacybescherming gaat een belangrijke rol spelen bij de gegevensuitwisseling bij het internet der dingen.
De vraag is echter in hoeverre de burger op privacy is gesteld en hoe hierbij de afweging wordt gemaakt over wat wel en wat niet nuttig is dat andere partijen (overheid, bedrijfsleven, medische zorg) over de burger weten. Een belangrijk uitgangspunt hierbij is dat burgers zelf moeten kunnen beslissen over wat anderen wel en niet over hen mogen weten. Vanuit dat gezichtspunt beschrijft Garfinkel (2008) privacy als:

> 'the right of people to control what details about their lives stay inside their own houses and what leaks to the outside'.

Malhotra,Kim en Agarwal (2004) onderscheiden drie belangrijke criteria die bij de borging van privacy als publiek belang gelden: (1) de gegevens worden op competente en betrouwbare wijze verzameld, (2) het is mogelijk de gegevens te controleren, en (3) de gebruiker is zich bewust van het mogelijke maatschappelijk belang van de gegevens. Bij dit alles is het natuurlijk essentieel dat de burger begrijpt waar de gegevens voor nodig zijn en hoe ze kunnen worden gebruikt en eventueel misbruikt. Dit sluit aan bij het eerdergenoemde opheffen van marktfalen van informatieasymmetrie. Het is nodig dat de burger de toegevoegde waarde inziet van diensten die dankzij de gegevens geleverd kunnen worden. Bovendien dient de burger te allen tijde de juistheid van de gegevens te kunnen controleren en ook te kunnen beslissen of de gegevens worden verzameld en, zo ja, aan wie ze ter beschikking mogen worden gesteld. Daartoe dienen de gebruikers van de gegevens transparant over dit gebruik te zijn en aan te geven wie over de gegevens de beschikking krijgt, dan wel aan wie de gegevens worden (door)verkocht. Al met al ligt het voor de hand dat de burger in die zin het eigendomsrecht van de persoonlijke gegevens verwerft (Pentland, 2009), dat altijd de mogelijkheid tot rectificatie van verkeerde gegevens wordt geboden. Immers, niet alleen misbruik van gegevens moet worden voorkomen, maar ook te goeder trouw gebruik van verkeerde gegevens. Dit laatste kan bij persoonsgerichte aanbiedingen of toegang tot kredietverlening al zeer hinderlijk zijn, maar bij medische zorg zelfs levensbedreigend.

 doi: 10.5553/BenM/138900692016043001004 - Beleid en Maatschappij 2016 (43) 1

Zeggenschap en het recht te vergeten

Het feit dat de burger zeggenschap over zijn gegevens moet blijven houden, maar dat de gegevens in hun totaliteit het karakter van een collectief goed kunnen hebben, stelt stringente eisen aan het ontwerp van de applicaties en systemen die via het internet der dingen gegevens opleveren. In beginsel dient dit te gebeuren via een vergunning, die de burger voor het gebruik van de gegevens verleent. Zo'n vergunning beschrijft wat de gebruiker wel en niet mag doen met de gegevens. Zo mag de gebruiker, afgezien van een nadrukkelijke toestemming door de burger, niet de persoonlijke gegevens doorverkopen, maar mag hij wel, bijvoorbeeld in het geval van bezoekgegevens aan een winkelcentrum, geaggregeerde gegevens over het bezoek aan het winkelcentrum en de karakteristieken van de bezoekers doorgeven. De verhandelbaarheid van de gegevens, zoals bepleit door Bijlsma en anderen, (2014), mag daarom uitsluitend betrekking hebben op deze geaggregeerde en geanonimiseerde gegevens. Het anonimiseren van gegevens stelt hoge eisen aan de manier waarop de gegevens worden samengevoegd. Een klein aantal karakteristieken is vaak al voldoende om individuele 'geanonimiseerde' gegevens tot individuen te kunnen herleiden. In de praktijk verleent de gebruiker van internet maar al te gemakkelijk toestemming voor gebruik en hergebruik van gegevens (Zuiderveen Borgesius, 2015). Bovendien gaat het bij de gespecialiseerde bedrijven die verschillende via internet verkregen persoonlijke gegevens aan elkaar koppelen en doorverkopen wel eens flink mis. Zo verhaalt Brian Krebs (2013) hoe de gegevensgigant Experian gegevens van consumenten heeft doorverkocht aan een Vietnamese dief van identiteiten. En dat terwijl Experian ook bescherming tegen een dergelijke diefstal van persoonsgebonden gegevens verkoopt.

Het verzamelen en opslaan van de gegevens dient in beginsel in gesloten netwerken te gebeuren. De beheerders van deze netwerken dragen de verantwoordelijkheid dat individuele gegevens niet tegen de wens van de desbetreffende burgers worden geopenbaard, maar dat wel zo veel mogelijk aan de vraag naar gegevens op geaggregeerd niveau wordt voldaan. Dit alles is gemakkelijker gezegd dan gedaan. Microsoft heeft een initiatief gesponsord om dit probleem van de bescherming van gegevens wereldwijd te bespreken (Cate & Mayer-Schönberger, 2013). Uit deze discussie komt naar voren dat licentieovereenkomsten waarschijnlijk de beste manier zijn om bescherming te bieden.

De manier waarop deze bescherming geëffectueerd moet worden, is vooral een technische kwestie. De ontwerper van de applicatie of het systeem waarbij apparaten met elkaar communiceren en gegevens opleveren, moet het voortouw nemen bij de inbouw van de beschermingsconstructies. Zo dient te worden nagedacht over hoe om te gaan met de wens van een burger om geen verdere individuele gegevens te verzamelen. Blijft het systeem dan nog wel bruikbaar? Volgens Weber (2010) zijn er allerlei Privacy Enhancing Technologies (PET's) beschikbaar, zoals: peer-to-peer netwerken, virtuele privénetwerken, Transport Layer Security-systemen, Domain Name System Security Extensions, Onion Routing Encryps en privé-informatiesystemen. Hoewel sommige PET's in bepaalde situaties een goede bescherming bieden, luidt de conclusie toch dat er altijd overheidsregulering nodig is om het publiek belang van de rechtsbescherming te borgen.

Deze rechtsbescherming betreft overigens niet alleen de privacy. Het is evenzeer van belang dat van buitenaf niet kan worden ingebroken in de communicatie tussen apparaten in het internet der dingen. Zo dient het natuurlijk onmogelijk te worden gemaakt dat derden bij jou via de slimme thermostaat de verwarming hoger gaan zetten. In die zin noemt Arnbak (2015) het incident waarbij beveiligingsonderzoekers van buitenaf een zichzelf besturende jeep konden doen afremmen en daarna via plankgas de greppel insturen. Het zijn de makers van de software die hier volgens Arnbak aansprakelijk voor moeten worden gesteld. Maar vanuit het perspectief van de borging van publiek belang is het de overheid die via regelgeving zo goed mogelijk dient te zorgen dat een dergelijke inbraak in de gegevensuitwisseling niet mogelijk kan zijn.

Veel problemen betreffende de privacybescherming hebben tegenwoordig betrekking op de sociale media (Livingstone, 2008). Hier is de tendens dat de burgers zich minder zijn gaan bekommeren om privacybescherming. Zie echter Goldfarb en Tucker (2012) voor een nuancering. Voor de ontwerper die de mogelijkheden van gegevensverzameling via het internet der dingen wil benutten, lijkt dit goed nieuws. Het verruimt de speelruimte. Maar het recht op privacy blijft onveranderlijk bestaan. Het betekent dat bij het ontwerp van nieuwe toepassingen van het internet der dingen er steeds beter op wordt gelet dat de communicatie geen grote persoonlijke schade kan berokkenen.

Vooralsnog heeft de regelgeving met betrekking tot de privacybescherming en, meer algemeen, het misbruik door derden van gegevensuitwisseling op internet – denk aan cybercrime – vooral betrekking op het gebruik van internet zelf. Recentelijk is er veel juridische aandacht geweest voor het beginsel van het 'recht op vergeten' waarover het Europees Hof van Justitie een uitspraak heeft gedaan (Raad voor de Leefomgeving en Infrastructuur, 2015, 30). De jurisprudentie tracht hier een goede middenweg te vinden tussen de mogelijkheid van burgers om toegang via zoekmachines tot onwelgevallige informatie te doen verwijderen, en de vrijheid van meningsuiting (Kulk & Zuiderveen Borgesius, 2015). Daarbij ligt de focus op de mogelijkheid van burgers om zoekmachines (met name Google) te verzoeken zoekresultaten met onwelgevallige informatie uit hun lijst te verwijderen. Daarnaast heeft het College bescherming persoonsgegevens (CBP) Google op de vingers getikt over het vanuit het oogpunt van privacy ongeoorloofd combineren van gegevens (zie de brief van CBP aan Google Inc. d.d. 9 juni 2015). Dit college ziet toe op de uitvoering van de Wet bescherming persoonsgegevens en is een onafhankelijke institutie waaraan de overheid de borging van het publiek belang van privacybescherming heeft gedelegeerd.

De regelgeving ten aanzien van rechtsbescherming bij het internet der dingen is echter nog weinig uitgekristalliseerd. Het onafhankelijke adviesorgaan van Europese toezichthouders op privacy – de Artikel 29-werkgroep – heeft in een opiniedocument (Article 29 Data Protection Working Party, 2014) aandacht besteed aan de grootste risico's die bij de ontwikkeling van het internet der dingen spelen en daarover richtlijnen aangegeven. Vooralsnog gaan deze richtlijnen uit van bestaande wetgeving. Een van de aanbevelingen is dat er Privacy Impact Assessments moeten worden uitgevoerd voor alle nieuwe applicaties waar de gegevensuitwisseling via het internet der dingen loopt. Daarbij zijn het de producenten

van de applicaties die als 'data controllers' onder de EU-wetgeving verantwoordelijk zijn voor de privacybescherming. Maar uiteindelijk is het de overheid, en zijn het in dit verband de afzonderlijke overheden van de EU-lidstaten, die vanuit de eigen voorkeur op basis van deze wetgeving en richtlijnen de privacybescherming dienen te borgen. Overigens klaagt Weber (2010, 29) dat de EU slechts een vaag kader voor de regelgeving verschaft, waarbij geen rekening wordt gehouden met vormen van standaardisatie en zelfregulering bij de producenten. Daarbij kan zelfregulering tot doel hebben om reputatieschade te vermijden en daarmee op volstrekt rationele argumenten berusten – buiten eventuele aanvullende ethische overwegingen. De reputatieschade voor bedrijven waarvan bekend is dat zij privacyregels hebben geschonden, kan namelijk flink in de papieren lopen (zie bijvoorbeeld Acquisti, Friedman & Telang, 2006).

Rol van opdrachtgever, ontwerper en programmeur

Het voorgaande maakt duidelijk dat flink wat overheidsbemoeienis in de vorm van regulering nodig is bij de borging van de publieke belangen bij het internet der dingen. Hier is nog veel werk aan de winkel, zowel op het gebied van privacybescherming als op het gebied van veiligheid en misbruik. Wat betreft de privacybescherming gaat het daarbij om gegevensgebruik door de overheid (WRR, 2011) en om bescherming tegen commercieel gebruik van big data (Lane e.a., 2014).
Wanneer de regels voor rechtsbescherming zijn vastgesteld, is er bij handhaving van deze regels sprake van de gebruikelijke relatie tussen principaal en agent (of opdrachtgever en opdrachtnemer). Hierbij is de overheid de 'principaal', en de eigenaar/beheerder van de applicatie of het systeem waarbij via internet apparaten met elkaar communiceren, de 'agent'. Gestreefd dient te worden naar een manier van borging waarbij de verschillende kosten – nalevingkosten, uitvoeringskosten en afstemmingsverlies – die de principaal-agentrelatie met meebrengt, zo klein mogelijk zijn (Den Butter, 2013). Vertrouwen in het toezicht op de regelgeving kan daarbij de kosten verlagen (Paauw-Fikkert, Six & Robben, 2014), zij het dat het veelal om een berekend vertrouwen (calculated trust) zal gaan waarbij de winst van de vertrouwensbreuk niet opweegt tegen het reputatieverlies van degene die het vertrouwen verbreekt. De principaal-agentrelatie veronderstelt dat de agent – in dit geval dus de eigenaar/beheerder ofwel de 'data controller' in het EU-jargon – meer informatie heeft over de manier waarop het publiek belang geborgd kan worden dan de principaal. Om verwarring te voorkomen zij opgemerkt dat het hier om informatieasymmetrie gaat tussen de eigenaar/beheerder van de applicatie of het systeem en de overheid als handhaver van regels. Dit is een andere informatieasymmetrie (en dus vorm van marktfalen) dan tussen burgers en gebruikers van big data bij verwerving en verwerking van die gegevens.
Handhaving van regels in dit geval van applicaties en systemen bij het internet der dingen levert een ingewikkelde principaal-agentrelatie op. Hier is het de ontwerper van de applicatie of het systeem die de meeste kennis heeft van hoe aan de regelgeving, bijvoorbeeld in het geval van privacybescherming, kan worden vol-

daan. Zo ontstaat een soort gestaffelde principaal-agentrelatie waarbij de eigenaar/beheerder van de applicatie of het systeem de zorg om aan de regelgeving te voldoen uitbesteedt aan de ontwerper. Of anders gezegd, in de opdracht aan de ontwerper moet zijn ingebouwd dat de ontwerper ervoor dient te zorgen dat de applicatie of het systeem aan de regels voldoet. Deze taakverdeling is te vergelijken met die bij regelgeving in de bouw, waarbij een bouwwerk dient te voldoen aan de bouwvoorschriften en dient te passen in het bestemmingsplan. Het is de architect die namens de eigenaar/opdrachtgever van het bouwwerk ervoor zorgt dat alle voorschriften worden nageleefd en dat de vergunningen worden verkregen.
Dit legt een belangrijke verantwoordelijkheid bij de ontwerper van applicaties of systemen die gebaseerd zijn op gegevensuitwisseling via internet. Een probleem daarbij is dat de ontwerper weliswaar goed zicht heeft op het vernieuwend karakter en de vormgeving van de applicatie of het systeem, maar de technische kennis ontbeert over hoe in complexe softwaresystemen daadwerkelijk aan de gestelde voorschriften en vereisten kan worden voldaan. Die kennis ligt bij de softwareontwikkelaars (Chen, Liu & Xie, 2012).

Ontwerpstrategieën
Er zijn twee ontwerpstrategieën mogelijk. De eerste strategie is een ideaaltypische waarbij de ontwerpers eerst een volledig ontwerp maken en de softwareontwikkelaars vervolgens het ontwerp operationeel maken. Dit is het geval wanneer het ontwerpproces van een nieuw systeem is ingericht volgens de stage-gatemethode (Cooper, Edgett & Kleinschmidt, 2002). Net als in de klassieke aanbodketen worden daarbij de verschillende stadia in het ontwerp achter elkaar volgtijdelijk doorlopen en wordt de ontwerpfase met een beslissingsfase afgesloten. De ontwerper voert dan de beide eerste fases van het proces uit, waarbij aan de hand van de wensen van de opdrachtgever de scope van het systeem wordt bepaald en de businesscase wordt opgesteld. Het ontwikkelen en het testen van het systeem gebeuren vervolgens door de ontwikkelaars.
Deze strategie is echter minder geschikt om te kunnen voldoen aan de voorschriften en vereisten van de regelgeving. Immers, de ontwerpers zijn bij het ontwerp niet in staat te overzien welke technische beperkingen ten aanzien van de software zich kunnen voordoen bij het vervullen van die vereisten. Daarom is een tweede strategie van samenwerking, waarbij de softwareontwikkelaars vanaf het begin bij het ontwerpproces betrokken worden, een betere manier om tot een ontwerp te komen dat vernieuwend en commercieel aantrekkelijk is, maar dat ook voldoet aan de vereisten van de privacybescherming (Wang e.a., 2002). Het valt te vergelijken met een architect die de aannemer die het bouwwerk moet uitvoeren direct al in het ontwerpproces betrekt. De architect heeft kennis van wat de klant wil, maar de aannemer heeft vaak meer kennis over beschikbaarheid van materialen en specifieke plaatselijke omstandigheden. In het stage-gatemodel is dit niet vanzelfsprekend. Dit zou betekenen dat bij ieder beslissingsmoment (gate) er een bijeenkomst zou moeten zijn met alle disciplines, die elkaar eerst op de hoogte moeten brengen van de processen waarmee ze bezig zijn. Zo kan er alleen tot op zekere hoogte betrokkenheid gecreëerd worden.

 doi: 10.5553/BenM/138900692016043001004 - Beleid en Maatschappij 2016 (43) 1

Een manier om vanaf de start van het project samen te werken is om het ontwerpproces vorm te geven in kleinere iteratieve fases van overleg tussen ontwikkelaars en ontwerpers. Dit geldt dan dus ook al in de fase waarin de functionele eisen voor het te maken systeem worden opgesteld. Een voordeel van zo'n ontwerpproces is dat via deze samenwerking tussen de ontwikkelaars en de ontwerpers snel concepten in prototypes kunnen worden omgezet. Immers, juist in de conceptfase worden de meest verstrekkende beslissingen over het ontwerp genomen (Wang e.a., 2002). Na verschillende iteraties en het doorlopen van verschillende concepten wordt uiteindelijk de beslissing genomen welk concept verder uitontwikkeld wordt tot het uiteindelijke systeem. In deze bijeenkomst wordt dan de uiteindelijke architectuur bepaald. Hierin wordt beschreven welke gegevens worden uitgewisseld en hoe dat gebeurt. Vanwege deze nauwe samenwerking tussen ontwerpers en softwareontwikkelaars krijgen de ontwerpers direct een beeld van wat de ontwerpbeslissingen betekenen voor de privacy van de gebruikers van de applicatie of het systeem. In die zin vervult dit samenwerkingsmodel een belangrijke rol bij een goede borging van het privacyaspect en het veiligheidsaspect van het publiek belang van het internet der dingen.
Dit ontwerpproces kan worden geschaard onder het 'agile' ontwikkelen van software. Het ontwerp wordt in interactie met de verschillende betrokkenen en soms zelfs met geselecteerde gebruikers opgezet en uitgewerkt. Een voorbeeld is de 'scrummethode'. Dit is een flexibele manier om (software)producten te maken, waarbij met multidisciplinaire teams in korte periodes, met een vaste lengte van één tot vier weken, intensief wordt gewerkt. De beschreven manier van samenwerking tussen de ontwerpers en ontwikkelaars zou goed binnen deze scrummethode van softwareontwikkeling geïmplementeerd kunnen worden. Overigens is de scrummethode (vernoemd naar een 'scrum' in een rugbywedstrijd) bij de ontwerpers van Apple en Google al volledig ingeburgerd (NRC Handelsblad, 2015, E10-E11). Deze methode is indertijd ontwikkeld door Takeuchi en Ikujiro (1986). Zie ook Schwaber en Sutherland (2013).

Voorbeeld: Toon®, de slimme thermostaat

Een voorbeeld van de rol van de ontwerper bij het internet der dingen vormt de release in januari 2014 van de slimme thermostaat Toon®, die door het Amsterdamse bedrijf Quby is ontwikkeld. Eneco stelt deze thermostaat ter beschikking aan haar afnemers van energie. Met Toon is het mogelijk via de mobiele telefoon op afstand de thermostaat te bedienen en bijvoorbeeld de verwarming in te schakelen wanneer men van plan is over een uur thuis te komen. Of men kan, bij overwerk of een onverwacht bezoek aan een café of het theater, de verwarming nog wat langer uitschakelen. Dit alles bevordert het efficiënt energieverbruik. Maar het verschaft aan de energieleverancier ook een schat aan gegevens over dit energieverbruik in relatie tot de persoonlijke levensomstandigheden. Aan de gebruikers van Toon is toegezegd dat zij elk kwartaal een nieuwe release krijgen waarin de mogelijkheden van Toon worden uitgebreid. In de release van januari 2014 kunnen de gebruikers dagelijks zien hoe hun verbruik zich verhoudt tot het ver-

bruik van andere Toon-gebruikers. Het stroom- en gasverbruik wordt vergeleken met soortgelijke huishoudens. Ook biedt deze release de mogelijkheid om het verbruik specifiek te vergelijken met vrienden die ook een Toon hebben door ze via Toon uit te nodigen. Hiermee kan als het ware een soort wedstrijd worden gehouden wie van de vrienden het meest zuinig is in het energieverbruik. De vormgeving op de display van Toon is erop gericht om deze vergelijking van energieverbruik zo inzichtelijk mogelijk te maken (zie figuur 1) Zo kan eenvoudig worden afgelezen wie van de vrienden zuiniger is en ook hoe het verbruik verloopt ten opzichte van gemiddelde en zuinige huishoudens. De grafieken in de display geven daarbij inzicht in hoeveel er mogelijk nog te besparen valt.
Twee aspecten van het publiek belang van het internet der dingen komen in deze release van Toon tezamen. In de eerste plaats beoogt Toon bij te dragen tot energiebesparing. Rosenkrantz, Muehlfeld en Dirkmaat (2013) geven een overzicht van de soortgelijke manieren waarbij gepoogd is met behulp van sociale normen en rangschikking tot een besparing van energiegebruik in huishoudens te komen. Allcott (2011) laat in dit verband zien dat het sturen van brieven waarin het energieverbruik met dat van de buren wordt vergeleken al tot een reductie van zo'n 2 procent van het energieverbruik kan leiden. Dat komt overeen met het effect van een prijsverhoging van 11 tot 20 procent op de korte termijn, en een prijsverhoging van 5 procent op de lange termijn. Het toont dat een dergelijke beïnvloeding van het gedrag, die ook de release van januari 2014 van Toon nastreeft, een substantiële bijdrage aan de vermindering van het energieverbruik kan leveren, die in plaats kan komen van een belastingverhoging op energie. In die zin kan Toon bijdragen aan het publiek belang van het internaliseren van de negatieve externe effecten van energieverbruik en milieubelasting. De effectiviteit van Toon hierbij dient nog nader te worden onderzocht. Een manier om dat te doen, zoals ook door Allcott (2011) gesuggereerd, is een 'verschil op verschil'-berekening te maken van het energieverbruik van klanten van Eneco die wel met vrienden vergelijken, en de klanten die niet actief gebruikmaken van de release van januari 2014.

Aan de andere kant levert de communicatie via internet tussen Toon en de gebruiker veel individuele gegevens op over de leefwijze van de gebruiker in relatie tot het energieverbruik. Het publiek belang hier is dat de privacy van de individuele gebruiker dient te worden beschermd. De softwarearchitectuur van Toon moet zodanig zijn ingericht dat deze gegevens niet voor andere doeleinden worden gebruikt dan voor datgene waarvoor de gebruiker toestemming heeft verleend. Zo mag Toon niet zelf bepalen wie de vrienden zijn met wie wordt vergeleken, maar dienen die 'vrienden' zich expliciet via een website aan te melden.
In de architectuur van deze applicatie, die mede door een van de auteurs van dit artikel is ontworpen, is rekening gehouden met de borging van de privacy en met het risico dat de gegevens worden misbruikt. De specifieke gegevens over het verbruik van de individuele gebruikers worden alleen opgeslagen op de hardware van Toon zelf. Eens per dag worden de gegevens over het gas- en stroomverbruik van het desbetreffende huishouden uitgelezen ten behoeve van de vergelijkfunctie. Om de vergelijking te maken met het gemiddelde verbruik worden deze gegevens

 doi: 10.5553/BenM/138900692016043001004 - Beleid en Maatschappij 2016 (43) 1

vergeleken met het gemiddelde van hetzelfde type huishouden in Nederland. Voor de optie waarbij een vergelijking met vrienden wordt gemaakt, worden geen specifieke verbruikersgegevens uitgelezen. De vergelijking komt tot stand met percentages, gerelateerd aan de verschillende energielabels. Als bijvoorbeeld huishouden X met stroomverbruik in de beste 20 procent van zijn peers in Nederland zit, krijgt het een energielabel A. Dit is ook het enige wat de vrienden kunnen zien (zie figuur 1). De vergelijking vindt dus plaats op basis van de labels die voor de vrienden gelden. Daarbij wordt tevens gecorrigeerd voor de periodes dat de gebruikers op vakantie zijn en het energieverbruik dus tijdens zo'n periode laag maar niet relevant is voor de vergelijking. Aldus is de wijze waarop de nieuwe release van Toon tot stand is gekomen en privacybescherming is ingebouwd te zien als een voorbeeld van de hiervoor besproken vorm van intensieve samenwerking tussen ontwikkelaars en ontwerpers. Het laat zien dat door slim de gegevens te verzamelen en bepaalde informatie te normeren, voorkomen kan worden dat specifieke gegevens van verbruikers nodig zijn. Zo wordt in dit voorbeeld de privacy van de gebruikers gewaarborgd. Opgemerkt zij dat dit niet een gevolg is van regelgeving door de overheid of van een uitwerking van de richtlijnen die de EU (later) ervoor heeft opgesteld. Borging vindt hier plaats vanuit intrinsieke motivatie van de opdrachtgever om geen reputatieschade op te lopen: dus een vorm van zelfregulering.

Besluit

Het internet der dingen biedt ongekende mogelijkheden voor het verzamelen van grote hoeveelheden gegevens (big data) die veelal een gedetailleerde inkijk bieden in de persoonlijke levenssfeer, gebruiken en voorkeuren van individuele burgers. Daarnaast heeft, aldus Blom (2015), het internet der dingen de belofte in zich voor een groot aantal productinnovaties te zorgen, zoals auto's die hun onderhoud zelf regelen of toepassingen voor veiligheid thuis. Het is evident dat met deze nieuwe mogelijkheden publieke belangen zijn gemoeid, zowel in positieve als in negatieve zin. Vooralsnog is weinig nagedacht over welke overheidsbemoeienis bij de borging van deze publieke belangen nodig is. Dit artikel geeft een aanzet vanuit de welvaartstheoretische argumenten die bij het benoemen van de verschillende publieke belangen gelden. Informatieasymmetrie en verschillende externe effecten duiden op marktfalen waar overheidsbemoeienis gewenst is. Vanuit het oogpunt van rechtszekerheid vormen privacybescherming en veiligheid een belangrijk te borgen publiek belang. De statistische informatie van de big data heeft ook op zichzelf het karakter van een collectief goed. Daarmee is de openbare toegang tot deze gegevens eveneens een publiek belang. Volgens Etzioni (2014) is het daarbij nodig dat een goede balans gevonden wordt tussen privacybescherming en de collectieve voordelen die internetgegevens bieden. Die balans dient wel voortdurend al naar gelang de omstandigheden te worden aangepast.
Vervolgens is ingezoomd op de rol van de ontwerper van de applicaties en systemen die gebruikmaken van de communicatie tussen apparaten op internet. For-

(bron: https://thuis.eneco.nl/~/media/eol/pdf/toon.../releasenotestoon26.ashx)

Figuur 1 ***Het display van Toon® bij een vergelijking van energieverbruik van Gijs met dat van Jesper***

meel is de eigenaar/beheerder van de applicatie of het systeem verantwoordelijk voor het voldoen aan de vereisten van overheidsregulering. In de principaal-agentrelatie tussen overheid en eigenaar/beheerder is het echter de ontwerper die de meeste informatie heeft over de meest adequate wijze om het publiek belang te borgen. De regelgeving zou zodanig moeten zijn dat de ontwerper ook de afgeleide verantwoordelijkheid over de borging krijgt, waarbij dit expliciet als contractvoorwaarde bij de opdrachtverlening geldt. Voor handhaving van deze regelgeving zou gebruikgemaakt kunnen worden van reputatiemechanismen, waarbij het zowel voor de ontwerper als voor de eigenaar/beheerder hoge kosten vanwege reputatieverlies betekent wanneer blijkt dat de regels zijn geschonden.
Deze handhaving kent nog flink wat onduidelijkheden. Zo is er een tendens bij gebruikers van internet om weinig beducht te zijn op privacy. Dat speelt bijvoorbeeld bij het gebruik van sociale media, waarbij vaak zeer gevoelige persoonlijke informatie virtueel op straat komt te liggen en verspreid kan worden zonder dat degene die het betreft daar controle over heeft (Humphreys, Gill & Krishnamurthy, 2010). De vraag is of de overheid op dit punt niet paternalistisch dient te zijn en de burgers tegen zichzelf in bescherming moet nemen. Vanuit de argumenten voor overheidsbemoeienis die de economische theorie van de collectieve

 doi: 10.5553/BenM/138900692016043001004 - Beleid en Maatschappij 2016 (43) 1

sector aandraagt, kan dit ook worden opgevat als de bemoeienis van de overheid om het marktfalen van onvolledige informatie te repareren.
Dit artikel betoogt dat bij de borging van het publiek belang van het internet der dingen het samenwerkingsmodel tussen ontwerpers en softwareontwikkelaars de voorkeur heeft. Op deze wijze wordt optimaal gebruikgemaakt van zowel de kennis van de ontwerper over de voorkeuren van de klanten als de technisch geavanceerde kennis van de softwareontwikkelaars over wat de beste manier is om gegevens voor misbruik of oneigenlijk gebruik af te schermen. Speciale aandacht verdient de vraag hoe er in het ontwerp rekening kan worden gehouden met storingen of onderbrekingen in het gebruik van applicaties of systemen. Zo kan een klant bijvoorbeeld de toestemming tot het verzamelen van bepaalde gegevens intrekken, maar hij kan ook zijn mobiele telefoon kwijtraken, zodat de gegevens in dat opzicht aan betrouwbaarheid verliezen. Een andere mogelijkheid is dat de klant geld zal gaan vragen voor het gebruik van zijn persoonlijke gegevens. Ook zo'n scenario zal in al zijn consequenties moeten worden doordacht in het ontwerp van de applicatie of het systeem. Al met al lijkt een verdere integratie van het internet der dingen in ons leven niet te stoppen, gezien de vele welvaartsvoordelen die het oplevert. Het vergt echter een goede afweging tussen deze baten en de welvaartskosten (Athey, 2014). Daarom is er snel een betere, op het internet der dingen gerichte regelgeving door de overheid nodig om uitwassen, zoals verbeeld in de film *Minority Report*, te voorkomen (Lane e.a., 2014).

Noten

1 www.youtube.com/watch?v=7bXJ_obaiYQ.

2 Zie www.smartplanet.com/blog/bulletin/by-2020-90-percent-of-cars-will-be-connected/.

Literatuur

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. *Proceedings of the Twenty-Seventh International Conference on Information Systems*.

Allcott, H. (2011). Social norms and energy conservation. *Journal of Public Economics*, 95 (9-10), 1082-1095.

Arnbak, A. (2015, 12 augustus). Internet: maak de makers van software aansprakelijk. *Het Financieele Dagblad*, p. 9.

Article 29 Data Protection Working Party (2014). *Opinion 8/2014 on the Recent Developments on the Internet of Things* (14/EN WP 223). European Commission, Directorate General Justice.

Athey, S. (2014). Information, privacy and the internet: an economic perspective. *CPB Lecture*, juni.

Bijlsma, M., Straathof, B., & Zwart, G. (2014). Kiezen voor privacy: hoe de markt voor persoonsgegevens beter kan. *CPB Policy Brief*, 4.

Blom, M. (2015). Laat die 'robots' als metafoor maar weer los. In: B. ter Weel (red.), *De match tussen mens en machine* (Preadviezen van de Koninklijke Vereniging voor de Staathuishoudkunde). Amsterdam, 43-52.

Bomhof, F. (2014). Big data: kleine data worden groot. *Christen Democratische Verkenningen*, herfst: 34-41.

Bovenberg, A.L., & Teulings, C.N. (1999). Op zoek naar de grenzen van de staat: publieke verantwoordelijkheid tussen contract en eigendomsrecht. In: W. Derksen e.a. (red.), *Over publieke en private verantwoordelijkheden* (WRR Voorstudies en Achtergronden V105). Den Haag: Sdu Uitgevers, 19-136.

Butter, F.A.G. den (2011). Marktwerking en het 'wat' en 'hoe' van het publiek belang. *Tijdschrift voor Openbare Financiën*, 43 (2): 78-92.

Butter, F.A.G. den (2013). The perspective of public sector economics on regulation: transaction costs and the agency model. In: A. Alemanno e.a. (red.), *Better Business Regulation in a Risk Society*. New York: Springer, 119-134.

Cate, F.H., & Mayer-Schönberger, V. (2013). Notice and consent in a world of Big Data. *International Data Privacy Law*, 3 (2): 67-73.

Chen, Y., Liu, Z.L. & Xie, Y.B. (2012). A knowledge-based framework for creative conceptual design of multi-disciplinary systems. *Computer-Aided Design*, 44 (2): 146-153.

Cooper, R.G., Edgett, S.J., & Kleinschmidt, E.J. (2002). Optimizing the stage-gate process: what best-practice companies do. *Research-Technology Management*, 45 (5): 21-27.

Etzioni, A. (2014). A cyber age privacy doctrine: a liberal communitarian approach. *I/S: A Journal of Law and Policy for the Information Society*, 10 (2): 641-669.

Evans, D. (2011). *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything*. Cisco Internet Business Solutions Group (IBSG).

Garfinkel, S. (2008). *Database Nation: the Death of Privacy in the 21st Century*. Sebastopol, CA: O'Reilly Media.

Giusto, D., Lera, A., Morabito, G., & Atzori, L. (2010). *The Internet of Things*. Berlijn/Heidelberg: Springer.

Goldfarb, A., & Tucker, C. (2012). Shifts in privacy concerns. *American Economic Review: Papers and Proceedings*, 102 (3): 349-353.

Humphreys, L., Gill, P., & Krishnamurthy, B. (2010). How much is too much? Privacy issues on Twitter. *Conference of International Communication Association, Singapore* (juni 2010).

Krebs, B. (2013). http://krebsonsecurity.com/2013/10/experian-sold-consumer-data-to-id-theft-service/, geraadpleegd op 13 december 2015.

Kulk, S., & Zuiderveen Borgesius, F. (2015). Freedom of expression and 'right to be forgotten' cases in the Netherlands after Google Spain. *European Data Protection Law Review*, 2015 (2): 113-125.

Lane, J., Stodden, V., Bender, S., & Nissenbaum, H. (red.) (2014). *Privacy, Big Data and the Public Good*. Cambridge: Cambridge University Press.

Livingstone, S. (2008). Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society*, 10 (3): 393-411.

Malhotra, N.K., Kim, S.S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. *Information Systems Research*, 15 (4): 336-355.

McKinsey Global Institute (2011). *Big Data: The Next Frontier for Innovation, Competition, and Productivity*. Juni.

NRC Handelsblad (2015, 24-25 januari). Scrum jij al? Bij Apple doen ze 't wel. *NRC Weekend*, E12-E13.

Paauw-Fikkert, L., Six, F., & Robben, P. (2014). Vertrouwen in toezichtbeleid. *Beleid en Maatschappij*, 41 (3): 185-204.

Pentland, A. (2009). Reality mining of mobile communications: Toward a new deal on data. *The Global Information Technology Report 2008-2009*.

Raad voor de Leefomgeving en Infrastructuur (2015). *Verkenning Technologische Innovaties in de Leefomgeving*. Den Haag.

Rosenkrantz, S., Muehlfeld, K.S., & Dirkmaat, T. (2013). Een zetje in de richting van energiebesparing. *Economisch Statistische Berichten, Dossier Gedragseconomie voor Milieubeleid*, 98 (46725): 48-54.

Schrijvers, E., Stam, E., Stellinga, B., & Vries, G. de (2010). Marktwerkingsdebat: hoe nu verder? *Beleid en Maatschappij*, 37 (3): 197-206.

Schwaber, K., & Sutherland, J. (2013). *The Scrum Guide™. The Definitive Guide to Scrum: the Rules of the Game*.

Takeuchi, H., & Ikujiro, N. (1986). The new product development game. *Harvard Business Review*, 64 (1): 137-146.

Teulings, C.N., Bovenberg, A.L., & H.P. van Dalen (2003). *De calculus van het publieke belang*. Den Haag: Kenniscentrum voor Ordeningsvraagstukken.

Wang, L., Shen, W., Xie, H., Neelamkavil, J., & Pardasani, A. (2002). Collaborative conceptual design - state of the art and future trends. *Computer-Aided Design*, 34 (13): 981-996.

Weber, R.H. (2010). Internet of Things-New security and privacy challenges. *Computer Law & Security Review*, *26* (1): 23-30.

Went, R., & Kremer, M. (2015). Hoe we robotisering de baas kunnen blijven. Inzetten op complementariteit. In: R. Went e.a., *De robot de baas*. Amsterdam: Amsterdam University Press, 23-46.

WRR (2000). *Het borgen van publiek belang* (Rapporten aan de Regering, nr. 56). Den Haag: Sdu Uitgevers.

WRR (2011). *iOverheid* (Rapporten aan de Regering, nr. 86). Amsterdam: Amsterdam University Press.

WRR (2012). *Publieke zaken in de marktsamenleving* (Rapporten aan de Regering, nr. 87). Amsterdam: Amsterdam University Press.

Zuiderveen Borgesius, F. (2015). Privacybescherming online kan beter; de mythe van de geïnformeerde toestemming. *Nederlands Juristenblad*, 14: 878-883.